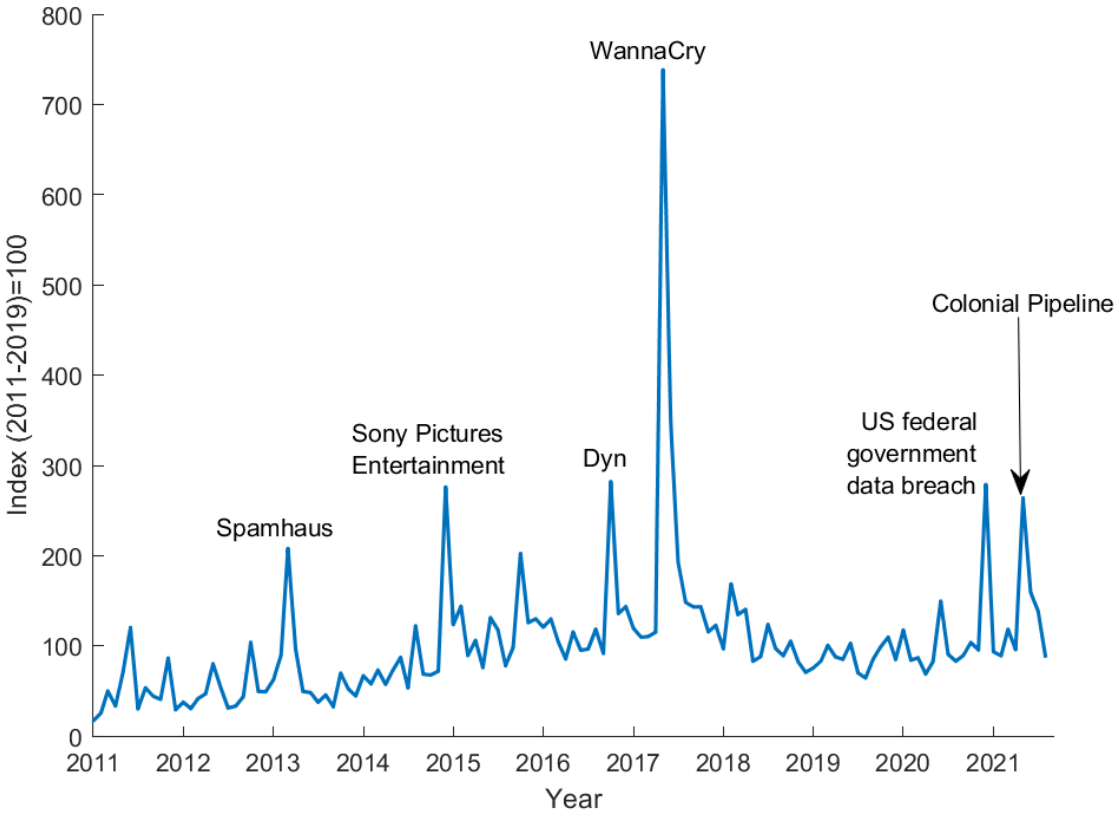
A measure of the evolution of cyber risk

By Stéphane Lhuissier and Fabien Tripier

After the 2008 financial crisis, then *the 2020 health crisis, will the next global economic crisis be a cyber crisis? Cyber risk is a real threat to the economy and public authorities are mobilised to deal with it. This post presents an indicator used to monitor this risk on a daily basis, based on exchanges on the social network Twitter.*

Chart 1 – Evolution of cyber risk over the last decade



Source: Twitter and authors' calculations.

With the digitisation and transformation of the economic and financial system, the risk of a major crisis emerging from cyberspace is to be taken seriously. This is what Christine Lagarde, President of the European Central Bank, suggested in her speech of 5 February 2020, as well as Jerome Powell, Chairman of the Federal Reserve of the United States on 12 April 2021. The latter declared: "*The chances that we would have a breakdown that looked anything like that [in 2008] are very, very low. The world evolves. And the risks change as well. And I would say that the risk that we keep our eyes on the most now is cyber risk*". In a 2019 systemic risk survey conducted by the Bank of England, 61% of respondents actually

expressed concern about the impact of cyber attacks on the financial system should they materialise, placing cyber risk ahead of geopolitical risk and the risk of a global economic slowdown.

Although cyber risk has gradually been taken into account in the governance and risk management framework of monetary and financial authorities (Kashyap and Wetherilt, 2019), the availability of cyber risk monitoring tools remains very limited (an exception is the study by Jamilov, Rey, and Tahoun, 2021, which offers a historical perspective on the evolution of cyber risk worldwide and within major economic sectors).

A tool for daily and real-time monitoring of cyber risk

In Lhuissier and Tripier (2021), we built a new indicator of cyber risk since 2011. The purpose of the indicator is to conduct a high-frequency, daily monitoring of cyber risk and an analysis of the different sectors of the economy concerned.

Cyber risk is defined as the combination of the probability of occurrence of cyber incidents (malevolent or non-malevolent incidents that threaten the cybersecurity of an information system or breach security procedures and rules) and their impact. In order to measure its evolution, we calculated the share of messages dedicated to cyber risk on the social network Twitter over the past ten years. More precisely, our indicator reflects the frequency of tweets, sent by English-speaking users, which contain the following words: "cyber" and "risk", "attack", or "threat". Our methodology has the following advantages: 1) it includes all the events that took place at the global level and gave rise to exchanges in English on this social network, 2) it weights the importance of one event relative to another (a major event will naturally be attributed more tweets than a minor one), and 3) it monitors the development of cyber risk on a daily basis and in real time. However, one must keep in mind the limitations of this indicator. It only covers the economic players present in this network, and moreover, they are English-speakers. In addition, we only measured the frequency of occurrence of keywords related to cyber risk, without analysing the content of the messages or the interactions of the senders of these messages.

Chart 1 shows the evolution of our cyber risk indicator from January 2011 to August 2021. The highest occurrence of messages related to cybersecurity on Twitter that we measured occurred in May 2017 during the WannaCry attack, a malware that hit hundreds of thousands of computers in hundreds of countries. The most recent major event that we identified is the May 2021 attack on Colonial Pipeline (the manager of an oil pipeline between Houston and New York) that had significant political repercussions (including the August 25 cybersecurity meeting hosted by President Joe Biden).

Certain events have repercussions on financial markets. As an example, in December 2020, the hack of SolarWinds, an IT management software company and supplier to US federal agencies and corporations, affected up to 18,000 customers and over 100 US companies. SolarWinds Corp. stock dropped by about 40% in just a few days following the attack. Although its effects did not cause any major incidents in the financial sector, such a scenario could occur in the future. Due to its very high level of digitisation and interconnection, the financial sector is particularly exposed to systemic risk, i.e. the consequences of a cyber

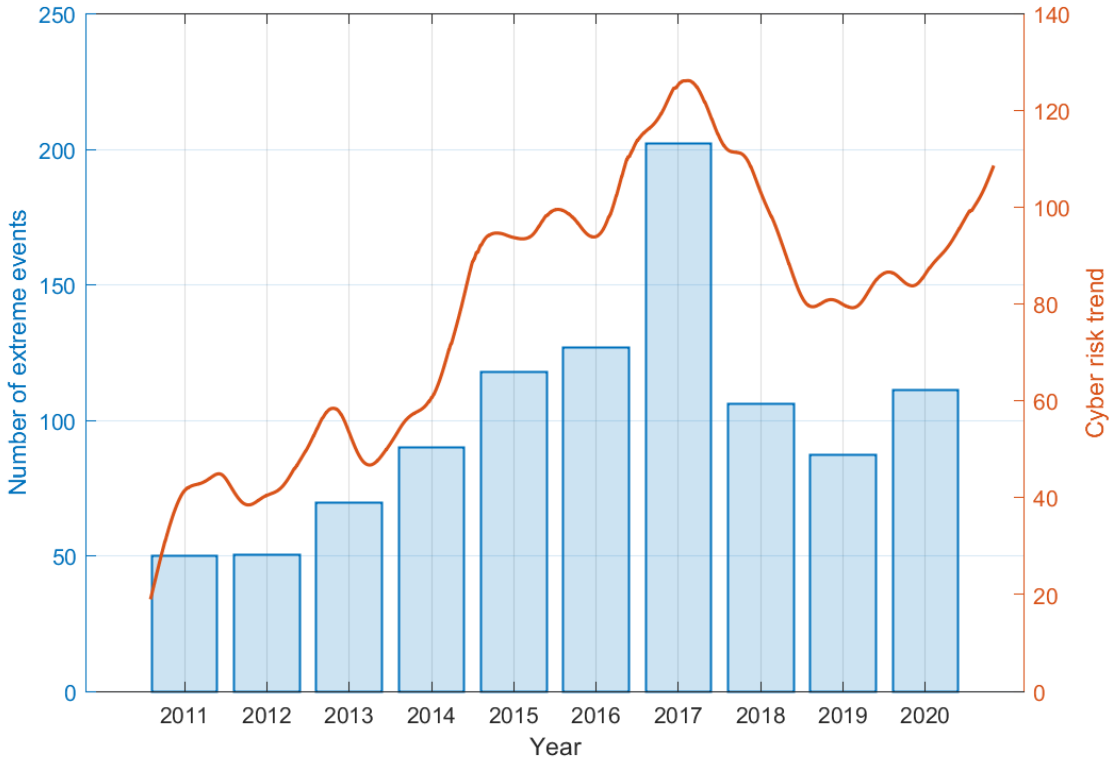
incident spread far beyond the initially impacted entity, causing damage to the economic and financial system as a whole.

A trend-cycle decomposition of cyber risk

The indicator provides a high-frequency, daily measure of cyber risk. However, it does not provide a clear view of its trend. In order to better understand the trend of cyber risk, Chart 2 shows the number of extreme events per year, defined here as the highest index values (top 5%), as well as the long-term trend of the index stripped of extreme events.

Between 2011 and 2017, the number of extreme events increased steadily, before dropping in 2018 and 2019, and rebounding in 2020. This evolution of cyber risk can also be observed through its long-term trend. Indeed, the trend shows that increasing attention was paid to cyber security until 2017; it then picked up again from 2020 in the context of the Covid-19 health crisis. These developments can be logically explained by the growing use of information technology and the transformations in the organisation of work and production, which are increasingly remote and connected.

Chart 2 – A worrying resurgence of cyber risk since the health crisis

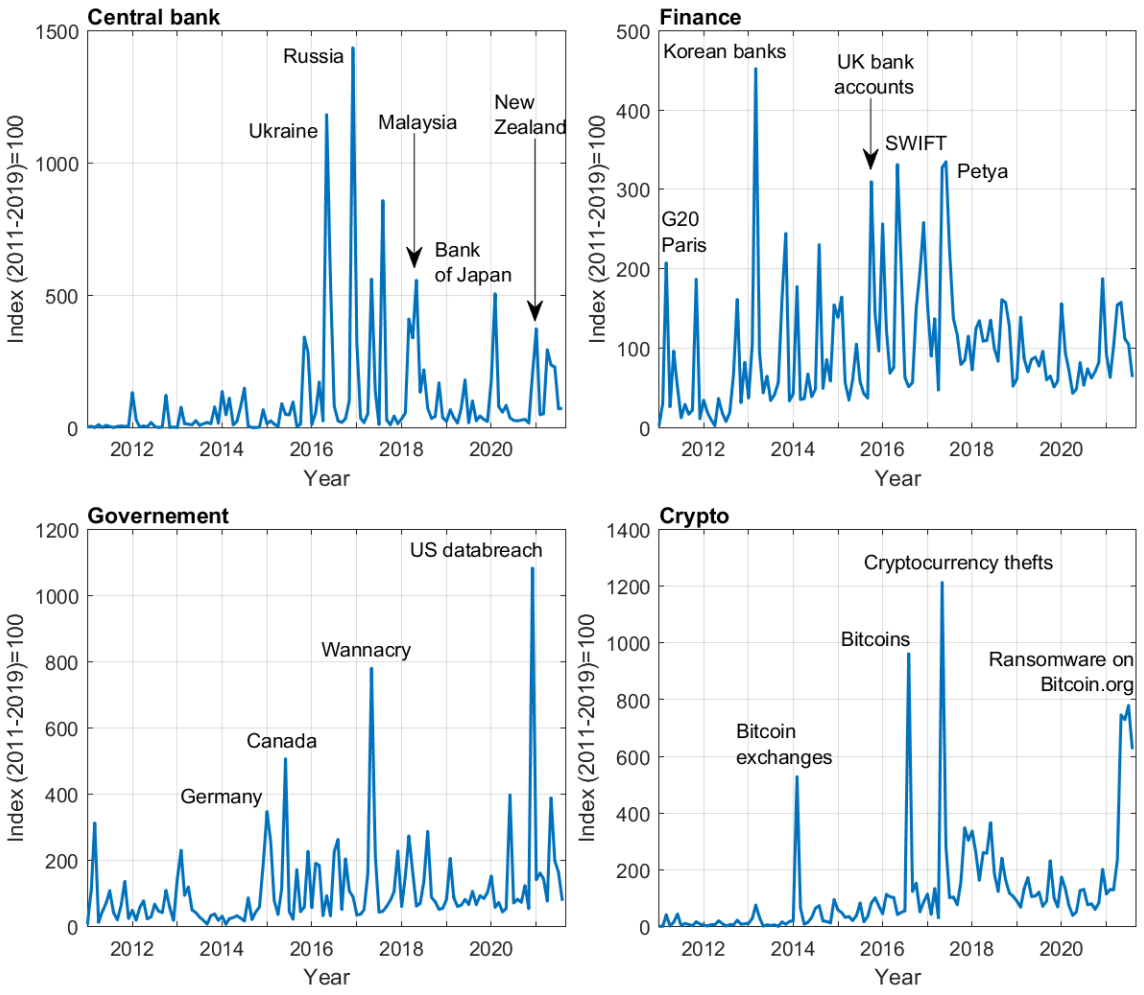


Source: Twitter and authors' calculations.

Sectoral indicators of cyber risk

In addition to our benchmark indicator, we developed indices for the sectors most exposed to cyber attacks by imposing more restrictive criteria when searching for tweets. For example, for an index specifically related to the financial sector, we searched for the following additional words: "bank," "bond," "financial market," "credit crunch," "currency," "debt," "dividend," "securities," and "finance."

Chart 3 – Sectoral indicators of cyber risk



Source: Twitter and authors' calculations.

Chart 3 shows an example of the sub-indicators studied in our analysis: central banks, finance, government agencies, and crypto-currencies. Each of these sectors are popular targets for cyber criminals as they hold a large amount of confidential and personal information. As an illustration, the cyber risk faced by central banks peaked with the 2016 attack on the Russian central bank, where hackers stole more than RUB 2 billion (EUR 24 million) from correspondent accounts. However, the spikes are not necessarily linked to the conduct of cyber attacks. For example, the indicator spiked in January 2020 when the Bank of Japan was concerned about the risk of cyber attacks before the Olympic Games kicked off. As another example, the cyber risk to which financial markets are exposed rose significantly

during major events, such as the attack on the G20 summit in Paris, the SWIFT network and the Petya ransomware in 2017. Chart 3 also shows a particularly worrying resurgence in cyber risk regarding crypto-currencies (this indicator is constructed by restricting the tweets in our benchmark indicator to those related to crypto-currencies). Crypto-asset exchange platforms are indeed subject to an increasing number of cyber attacks (e.g., the Bitcoin.org platform in July 2021).

Although cyber attacks have not yet led to a global economic and financial crisis, some cyber incidents could nevertheless affect our economies in the future, as in the scenarios studied by the European Systemic Risk Board (February 2020 report). Cyber risk is not only an IT security issue. It is therefore important to integrate and analyse it in the framework of macroeconomic and financial risk monitoring.